UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/803,788 | 03/17/2004 | Hristo Iankov Bojinov | 112056-0474 | 8050 |

24267        7590        07/08/2009
CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

| EXAMINER |
|---|
| COLAN, GIOVANNA B |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2162 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/08/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## DETAILED ACTION

1.      This action is issued in response to the Amendment filed on 04/21/2009.

2.      Claims 1, 31, 32, 38, 39, 45, 51, 52, 58, 59, 60, 61, 64, and 65 were amended.

Claims 6-29 were canceled. Claims 66-67 were added.

3.      Claims 1 –5, and 30 – 67 are pending in this application.


### *Response to Arguments*

4.      Applicant's arguments with respect to claims 1 –5, and 30 – 67 have been

considered but are moot in view of the new ground(s) of rejection.


### *Claim Rejections - 35 USC § 103*

5.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.      Claims 1 –5, and 30 – 67 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Chandrashekhar et al. (Chandrashekhar hereinafter) (2005/0033988

A1) in view of Ryuutou et al. (Ryuutou hereinafter) (US 2002/0083191).


        Regarding Claim 1, Chandrashekhar discloses a method for establishing identity

in a file system, comprising:

receiving a file request concerning an indicated file from a client, the request

received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the request from the proxy to a file server (Page 4, [0062] - [0065],

Chandrashekhar);

returning a reply associated with the file request from the file server to the proxy

(Page 4, [0066], Chandrashekhar);

inserting, by the proxy, metadata into a file handle (Page 3 and 4, [0055], "The

directed proxy server is adapted to provide policy information on either or both the

header information and the trailer information...", and [0067] – [0069]; respectively,

Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar)

Chandrashekhar also discloses sending, by the proxy the file handle to the client

(Page 4, [0070], Chandrashekhar).  However, Chandrashekhar does not explicitly

disclose sending, by the proxy, the file handle with the metadata inserted in the file

handle to the client.  On the other hand, Ryuutou discloses: inserting, by the proxy,

metadata into the file handle ([0072], and [0073], Ryuutou); and sending, by the proxy,

the file handle with the metadata inserted in the file handle to the client, the metadata to

be used in further requests to identify the client and the indicated file ([0074], Ryuutou).

It would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify Chandrashekhar by incorporating the step of sending, by the proxy,

the file handle with the metadata inserted, in the same conventional manner as

disclosed by Ryuutou. Skilled artisan would have found it motivated to use such a

modification in order to improve the response performance of a CORBA communication

using the HTTP tunneling by making a communication corresponding to a
communication connection request from a client within one session via the same
different Web server, in view of the above described problem (see; [0016], Ryuutou).

With respect to claims 32, and 38, the claims are rejected under the same
grounds as claim 1. Additionally, the combination of Chandrashekhar in view of
Ryuutou discloses "wherein the reply includes a file handle associated with the
indicated file (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar;
and Page 3, [0053], Ryuutou) as recited in claims 32 and 38.

Regarding Claims 2, 34, 47, and 60, the combination of Chandrashekhar in view
of Ryuutou discloses a method, further comprising the step of:
using the metadata in the file handles for any of eliminating a need for the proxy
to generate additional requests to the server to establish file identity, and for completing
client requests (Page 4, [0085], Chandrashekhar; and [0072], [0073], [0074],
"…subsequent communication connection requests…", Ryuutou).

Regarding Claims 4, and 36, the combination of Chandrashekhar in view of
Ryuutou discloses a method, further comprising:
using an NFS file system as the file system (Page 3, [0037], Chandrashekhar).

Regarding Claims 5, and 37, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

using a stateless protocol by the file system (Page 3, [0037], Chandrashekhar).


Regarding Claims 30, and 33, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

receiving, from the client, a second file request by the proxy (Page 4, [0061], Chandrashekhar), the second file request including the metadata in a further file handle sent with the second request (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], Ryuutou);

identifying, in response to the metadata, the client as  to submit the second file request (Page 4, [0068], Chandrashekhar);

sending the second file request to the file server and not sending the metadata with the second file handle to the file server (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

receiving by the proxy the further reply from the file server, and sending by the proxy the further reply to the client (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claim 31, the combination of Chandrashekhar in view of Ryuutou

discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file

request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] -

[0065], Chandrashekhar);

returning a reply associated with the first file request from the file server to the

proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle

associated with the indicated file (Figure 7, item: "Receiving file data from NAS server",

Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, metadata into the file handle (Page 3 and 4, [0055] and

[0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078],

Chandrashekhar);

sending, by the proxy, the file handle with the metadata inserted in the file handle

to the client, the metadata to be used in further requests to identify the client as having

a permission to access the indicated file ([0009], "The method includes requesting for a

file from a client to the proxy server and authenticating a requesting user of the client",

Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent

communication connection requests…", Ryuutou);

receiving, from the client, a second file request by the proxy (Page 4, [0061],

Chandrashekhar), the second file request including the metadata in a further file handle

sent with the second request (Page 3 and 4, [0055] and [0067] – [0069]; respectively,

Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

identifying, in response to the metadata, that the client has the permission to submit the second file request ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

sending the second file request to the file server and not sending the metadata with the second file handle to the file server (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

receiving by the proxy a second reply from the file server, and sending by the proxy the second reply to the client (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).


Regarding Claims 39, and 45, the combination of Chandrashekhar in view of Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

granting permission for the request to be acted upon by the file system in response to a predetermined protocol ([0009], "The method includes requesting for a file

from a client to the proxy server and authenticating a requesting user of the client",

Page 4, [0068], Chandrashekhar);

   returning a reply associated with the first file request from the file server to the

proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle

associated with the indicated file (Figure 7, item: "Receiving file data from NAS server",

Chandrashekhar; and Page 3, [0053], Ryuutou);

   inserting, by the proxy, a session key into the file handle (Page 3 and 4, [0055]

and [0067] – [0069]; respectively, Chandrashekhar; and also see Page 4, [0077] and

[0078], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication

connection requests…", Ryuutou); and

   sending, by the proxy, the file handle with the session key inserted in the file

handle to the client, the session key to be used in further requests to identify the client

and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074],

"…subsequent communication connection requests…", Ryuutou).


   Regarding Claims 40, and 46, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

   receiving, from the client, a second file request by the proxy (Page 4, [0061],

Chandrashekhar), the second file request including the session key in a second file

handle sent with the second file request ([0009], "The method includes requesting for a

file from a client to the proxy server and authenticating a requesting user of the client",

Page 4, [0068], Chandrashekhar; and [0072], [0073], [0074], "…subsequent

communication connection requests…", Ryuutou);

sending the second file request to the file server and not sending the session key

with the second file handle to the file server (Page 4, [0070], Chandrashekhar; and

[0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

and

receiving by the proxy a second reply from the file server, and sending by the

proxy the second reply to the client (Page 4, [0070], Chandrashekhar; and [0072],

[0073], [0074], "…subsequent communication connection requests…", Ryuutou).


Regarding Claims 43, and 49, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

using a NFS protocol as the predetermined protocol (Page 3, [0037],

Chandrashekhar).


Regarding Claims 44, and 50, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

using as the predetermined protocol a two way communication exchange

between the proxy and the file server (Fig. 1, Chandrashekhar).


Regarding Claim 51, the combination of Chandrashekhar in view of Ryuutou

discloses an apparatus to establish identity in a file system, comprising:

a proxy configured to receive a first file request sent by a client to a file system, the proxy further configured to forward the first file request to a file server (Page 4, [0059] - [0061], Chandrashekhar);

the file server configured to return a reply associated with the first file request to the proxy (Page 4, [0066], Chandrashekhar);

the proxy further configured to insert a session key into a file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar);

the proxy further configured to send the file handle with the session key inserted in the file handle to the client, the session key configured to be used in a second file request to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

the proxy further configured to receive, by the client, a second file request (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar), the second file request configured to include the session key in a second file handle sent with the second file request ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

the proxy further configured to receive the second file request, and the proxy to identify, in response to the session key, the client having a permission to submit the second file request, and the proxy to send the second file request to the file server and

not to send the session key with the second file handle to the file server ([0009], "The

method includes requesting for a file from a client to the proxy server and authenticating

a requesting user of the client", Page 4, [0085] and [0059], Chandrashekhar; and

[0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

and

the proxy further configured to receive a second reply from the file server, and

the proxy further configured to send the second reply to the client (Page 4, [0070],

Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection

requests…", Ryuutou).


Regarding Claims 52, and 58, the combination of Chandrashekhar in view of

Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file

request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] -

[0065], Chandrashekhar);

determining that the client has a permission to have the request acted upon by

the file system in response to a predetermined protocol ([0009], "The method includes

requesting for a file from a client to the proxy server and authenticating a requesting

user of the client", Page 4, [0068], Chandrashekhar);

returning a reply associated with the first file request from the file server to the

proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle

associated with the indicated file (Figure 7, item: "Receiving file data from NAS server",

Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, a cryptographic information into the file handle (Page 3

and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar; and also see Page 4,

[0077] and [0078], Chandrashekhar);

sending, by the proxy, the file handle with the cryptographic information inserted

in the file handle to the client, the cryptographic information to be used in one or more

requests to identify the client and the indicated file (Page 4, [0070], Chandrashekhar;

and [0072], [0073], [0074], "...subsequent communication connection requests...",

Ryuutou).


Regarding Claims 53, and 59, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

receiving, by the client, a second file request by the proxy, the second file

request including the cryptographic information in a second file handle sent with the

second file request (Page 3 and 4, [0055] and [0067] – [0069]; respectively,

Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072],

[0073], [0074], "...subsequent communication connection requests...", Ryuutou);

identifying, in response to the cryptographic information, that the client has

permission to submit the second file request ([0009], "The method includes requesting

for a file from a client to the proxy server and authenticating a requesting user of the

client", Page 4, [0068], Chandrashekhar);

sending the second file request to the file server and not sending the

cryptographic information with the second file handle to the file server (Page 4, [0070],

Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection

requests…", Ryuutou); and

receiving by the proxy a second reply from the file server, and sending by the

proxy the second reply to the client (Page 4, [0070], Chandrashekhar).


Regarding Claims 56, and 62, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

using a NFS protocol as the predetermined protocol (Page 3, [0037],

Chandrashekhar).


Regarding Claims 57, and 63, the combination of Chandrashekhar in view of

Ryuutou discloses a method according, further comprising:

using as the predetermined protocol a two way communication exchange

between the proxy and the file server (Fig. 1, Chandrashekhar).


Regarding Claim 64, the combination of Chandrashekhar in view of Ryuutou

discloses an apparatus to establish identity in a file system, comprising:

a proxy configured to receive a first file request sent by a client to the file system, the proxy to forward the first file request to a file server (Page 4, [0059] - [0061], Chandrashekhar);

the file server configured to return a reply associated with the first file request to the proxy (Page 4, [0066], Chandrashekhar);

the proxy further configured to insert a cryptographic information into a file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar);

the proxy further configured to send the file handle with the cryptographic information inserted in the file handle to the client, the cryptographic information configured to be used in a second file request to identify the client and the indicated file (Page 4, [0070], Chandrashekhar);

the proxy further configured to receive, by the client, a second file request, the second file request configured to include the cryptographic information in a second file handle sent with the second file request (Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

the proxy further configured to identify the second file request, in response to the cryptographic information, the client as having a permission to submit the second file request (Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

the proxy further configured to send the second file request to the file server and

not to send the cryptographic information with the second file handle to the file server

([0009], "The method includes requesting for a file from a client to the proxy server and

authenticating a requesting user of the client", Page 4, [0085] and [0059],

Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection

requests…", Ryuutou); and

the proxy further configured to receive a second reply from the file server, and

the proxy to send the second reply to the client (Page 4, [0070], Chandrashekhar).


Regarding Claim 65, the combination of Chandrashekhar in view of Ryuutou

discloses a method for establishing identity in a file system, comprising:

receiving a file request concerning an indicated file from a client, the request

received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the request from the proxy to a file server (Page 4, [0062] - [0065],

Chandrashekhar);

returning a reply associated with the file request from the file server to the proxy

(Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle associated

with the indicated file (Figure 7, item: "Receiving file data from NAS server",

Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, metadata into the file handle (Page 3 and 4, [0055] and

[0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078],

Chandrashekhar; and [0072], [0073], Ryuutou); and

sending, by the proxy, the file handle with the metadata inserted in the file handle to the client, a size of the file handle set to a sum of a length of the server file handle and a length of the proxy metadata ([0012], and [0038], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou), the metadata to be used in further requests to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claim 67, and 66, the combination of Chandrashekhar in view of Ryuutou discloses a computer apparatus, comprising:

a proxy configured to receive a client file request for a file (Page 4, [0059] - [0061], Chandrashekhar) and forward the file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

the server configured to return a reply associated with the file request (Page 4, [0066], Chandrashekhar), wherein the reply includes a file handle (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

the proxy further configured to intercept the file handle sent from the server and insert metadata into the file handle to create a modified file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], Ryuutou);

the proxy further configured to send the modified file handle with the metadata

inserted in the file handle to the client ([0012], and [0038], Chandrashekhar; and [0072],

[0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

the proxy further configured to receive the modified file handle from the client for

a second file request for the file, wherein the proxy is further configured to use the

modified file handle to eliminate a need for the proxy to generate one or more additional

requests to the server that would be required to access the file if the modified file handle

did not include the inserted metadata (Page 4, [0070], Chandrashekhar; and [0072],

[0073], [0074], "…subsequent communication connection requests…", Ryuutou).


Regarding Claims 3, and 35, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

encoding metadata in a form of a session key into the file handle, the session key

expiring after a predetermined amount of time ([0057 – [0059], Ryuutou).


Regarding Claims 41, and 48, the combination of Chandrashekhar in view of

Ryuutou discloses a method according to claim 39, further comprising:

causing the session key to expire after a selected amount of time ([0057 –

[0059], Ryuutou).


Regarding Claims 42, the combination of Chandrashekhar in view of Ryuutou

discloses a method, further comprising:

causing the session key to expire after a selected amount of usage ([0057 –

[0059], Ryuutou).


Regarding Claims 54, and 61, the combination of Chandrashekhar in view of

Ryuutou discloses a method, further comprising:

causing the cryptographic information to expire after a selected amount of time

([0057 – [0059], Ryuutou).


Regarding Claim 55, the combination of Chandrashekhar in view of Ryuutou

discloses a method, further comprising:

causing the cryptographic information to expire after a selected amount of usage

([0057 – [0059], Ryuutou).


### *Response to Arguments*

7.     Applicant argues that the applied art fails to disclose: "inserting, by the proxy,

metadata into a file handle; and sending, by the proxy, the file handle with the metadata

inserted in the file handle to the client, the metadata to be used in further requests to

identify the client and the indicated file".

Examiner respectfully disagrees.  the combination of Chandrashekhar in view of

Ryuutou does disclose: inserting, by the proxy, metadata into the file handle (Page 3

and 4, [0055], "The directed proxy server is adapted to provide policy information on

either or both the header information and the trailer information...", and [0067] – [0069];

respectively, Chandrashekhar and also see Page 4, [0077] and [0078],

Chandrashekhar; and [0072], and [0073], Ryuutou); and sending, by the proxy, the file

handle with the metadata inserted in the file handle to the client, the metadata to be

used in further requests to identify the client and the indicated file ([0074], Ryuutou).

See also rejection of claims 1, 32, and 38 discussed in this Office Action above.


8.      Applicant's arguments that; "Chandreshekhar explicitly teaches away from

Applicant's claimed sending the file handle with the metadata inserted in the file handle

to the client…" have been fully considered but they are not persuasive.

        As discussed above, the prior art Chandrashekhar does disclose: inserting, by

the proxy, metadata into the file handle (Page 3 and 4, [0055], "The directed proxy

server is adapted to **provide policy information on either or both the header

information and the trailer information**...", and [0067] – [0069]; respectively,

Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar).

        Additionally, the court upheld the rejection concluding that applicant's argument

that the reference teaches away from using epoxy was insufficient to overcome the

rejection since "Gurley asserted no discovery beyond what was known in the art." 27

F.3d at 554, 31 USPQ2d at 1132.). Furthermore, "[t]he prior art's mere disclosure of

more than one alternative does not constitute a teaching away from any of these

alternatives because such disclosure does not criticize, discredit, or otherwise

discourage the solution claimed…." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d

1141, 1146 (Fed. Cir. 2004).

### *Points Of Contact*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GIOVANNA COLAN whose telephone number is (571)272-2752. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Giovanna Colan
Examiner
Art Unit 2162


    /Jean B. Fleurantin/
    Primary Examiner, Art Unit 2162